2009-12

Cross network information sharing for handheld device based distributed system.

Chey Hock, Sim

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CROSS NETWORK INFORMATION SHARING FOR HANDHELD DEVICE BASED DISTRIBUTED SYSTEM

by

Lee Hong Aik
Sim Chey Hock

December 2009

Thesis Advisor:	Gurminder Singh
Second Reader:	Arijit Das

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2009	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Cross Network Sharing for Handheld Device Based Distributed System			**5. FUNDING NUMBERS**
6. AUTHOR(S) Lee Hong Aik, Sim Chey Hock			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**
13. ABSTRACT (maximum 200 words) TwiddleNet leverages on smart phones to facilitate information sharing among first responder teams during humanitarian aid and mass casualty scenarios. Situational awareness and relief efforts coordination can thus be derived from the timely and shared information. In view of large-scale disaster relief efforts, TwiddleNet is likely to operate in multiple sites with unique network establishments. The thesis focuses on testing various scenarios for cross-network, information-sharing operations. A new architecture, based on the study of the Nokia Mobile Server concepts and existing TwiddleNet operating models, is suggested in the thesis as well.			
14. SUBJECT TERMS TwiddleNet, Mobile Web Server, Cross Network Information Sharing			**15. NUMBER OF PAGES** 71
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

CROSS NETWORK INFORMATION SHARING FOR HANDHELD DEVICE BASED DISTRIBUTED SYSTEM

Hong Aik Lee
Civilian, Singapore Technologies Engineering Ltd, Singapore
B.Eng., (Hons), Nanyang Technological University, 2001

Chey Hock Sim
Civilian, Defence Science and Technology Agency, Singapore
B.Eng., (Hons), Nanyang Technological University, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
December 2009

Author: Chey Hock, Sim
Hong Aik, Lee

Approved by: Gurminder Singh
Thesis Advisor

Arijit Das
Second Reader

Peter J. Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

TwiddleNet leverages on smart phones to facilitate information sharing among first responder teams during humanitarian aid and mass casualty scenarios. Situational awareness and relief efforts coordination can thus be derived from the timely and shared information. In view of large-scale disaster relief efforts, TwiddleNet is likely to operate in multiple sites with unique network establishments. The thesis focuses on testing various scenarios for cross-network, information-sharing operations. A new architecture, based on the study of the Nokia Mobile Server concepts and existing TwiddleNet operating models, is suggested in the thesis as well.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACRONYMS	DEFINITION
C2	Command and Control
COTS	Commercial off-the-shelf
DHCP	Dynamic Host Configuration Protocol
HFN	Hastily Formed Network
HQ	Headquarters
HTTP	Hypertext Transmission Protocol
IP	Internet Protocol
LAN	Local Area Network
MWS	Mobile Web Server
NPS	Naval Postgraduate School
PDA	Personal Digital Assistant
TNT	Tactical Network Topology
TOC	Tactical Operations Centre
Wi-Fi	Wireless Fidelity

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to express thanks to many individuals who have influenced and assisted us during the writing of this thesis in many ways.

Many thanks to our thesis supervisors, Prof. Gurminder Singh and Arijit Das, for their valuable advice and guidance.

Thanks, also, to John Gibson for giving us the opportunity to perform TwiddleNet onsite testing using the TNT network infrastructure in Camp Roberts. His support has been invaluable in our test setup, both in the lab and on site.

We also wish to thank our sponsors, the Defence Science and Technology Agency (DSTA) and Singapore Technologies Engineering (STE), for making our studies at the Naval Postgraduate School possible.

Last, but not least, we would like to express our appreciation to our families and friends, both in Monterey and in Singapore, for their patience and support.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

TwiddleNet leverages the mobility of handheld wireless communication devices to reach out to any operation site with the objective of creating situation awareness. It is most useful for first-responder networking and information-sharing tasks that require immediate content capture and dissemination [1].

In 2005, the Category 5 hurricane, Katrina, caused severe destruction over 90,000 square miles of Louisiana and Mississippi. As the affected area was vast, there was a need for multiple responder teams (firefighters, police officers, medics) to be deployed over different disaster sites. Under such situations, it is only logical that information should be shared among the responder teams within and between sites throughout the entire operation. This would facilitate comprehensive situational awareness for better decision making and resources TwiddleNet is, therefore, a useful tool for deployment in this type of operation. However, TwiddleNet must be able to deploy at multiple sites to cover the ranges beyond the reach of a single site. This means that TwiddleNet must be able to operate across networks for information sharing. By allowing TwiddleNet to share information across networks, it will expand the capability of TwiddleNet to operate over a longer range and in larger areas of operation.

In deploying TwiddleNet across multiple networks, there is a high possibility that it will ride on established networks. Therefore, it is also important that the architecture of TwiddleNet have the flexibility to configure and work with the existing infrastructure.

A. OBJECTIVES

The aim of this thesis is to expand the existing TwiddleNet architecture for use in a multi-network environment and conduct tests to verify that this architecture can perform cross-network information sharing. Given the fact that TwiddleNet uses wireless IP-based architecture, TwiddleNet can be deployed across multiple networks that have access points to connect to. Investigations will determine the possibility of sharing information among TwiddleNet clients residing in different networks. Commercial off-the-shelf implementation will be explored in this thesis to bridge any gaps for cross-network information sharing.

This thesis will also perform a study of the Nokia Mobile Web Server and propose a possible future architecture for TwiddleNet. This architecture will combine the good features of both the Mobile Web Server and TwiddleNet, and, hopefully, will also eliminate the shortcomings of TwiddleNet.

B. RESEARCH QUESTIONS

The thesis will try to address the following research questions. 1) Is the existing TwiddleNet Architecture suitable for use in a multi-network environment? 2) How can information be stored and disseminated across different networks? 3) What are the best techniques to achieve information sharing across different networks using existing TwiddleNet Architecture? 4) Is there a need for totally new TwiddleNet architecture and concepts given the current technology trends?

C. SCOPE AND METHODOLOGY

There are two major scopes for the thesis. The first major scope will focus on reviewing the TwiddleNet system architecture and expanding the system capabilities to allow cross-network information sharing. Efforts are concentrated on reviewing the current TwiddleNet system architecture to determine gaps for cross-network information sharing. TwiddleNet system architecture is then evaluated for cross-network sharing feasibility. Given the advancement of technologies and trends in the last couple of years, this research hopes to bring together the next generation of TwiddleNet architecture. The thesis research will be conducted in three distinct phases.

1. Phase 1: Review of Current System Architecture

The first phase reviews the existing TwiddleNet system architecture. This involves reviewing the hardware configuration, network and software designs. The purpose is to identify technical shortfalls in the system for cross-network information sharing.

2. Phase 2: Test and Evaluate

Once the gaps in the system are identified, the next step is to research and design a solution to bridge the gaps. Subsequently, testing and evaluation can be done to verify the feasibility of cross-networking content sharing.

3. Phase 3: Propose a New Architecture for the Future Generation of TwiddleNet

TwiddleNet has been in operation for over two years. In the meantime, new technologies and wireless content-sharing concepts have evolved extensively. The final phase of the thesis will involve the study of current technologies. A new architecture for the next generation of TwiddleNet is then proposed following the study outcomes.

D. ORGANIZATION

This thesis is structured according to the following topics:

Chapter II explains the current architecture of TwiddleNet. TwiddleNet system components: Portal, Command Center and Mobile Clients roles and modes of operations are discussed. The limitations of the existing architecture are highlighted as well.

Chapter III discusses some design considerations for TwiddleNet to be deployed in multiple networks.

Chapter IV explains various test setups to verify the possibility of TwiddleNet to operate on multiple networks where cross-network information sharing can be achieved.

Chapter V proposes the next generation of TwiddleNet using Mobile Web Server concepts to bridge the existing gaps. The new TwiddleNet will harness all the desirable features of Mobile Web Servers and existing TwiddleNet to serve as a more effective tool for its intended purposes.

Chapter VI concludes this thesis with the findings from various lab and onsite testing.

E. BACKGROUND

Existing TwiddleNet architecture allows real-time information to be shared seamlessly between TwiddleNet hosts within a single network. This architecture has a restriction for operating over a large area as the range of deployment is as far as a single network can reach. In responding to an emergency situation such as a hurricane, TwitterNet is likely to deploy TwiddleNet at different networks that are interconnected to cover a large affected area. As such, situational content sharing can only be fulfilled if TwiddleNet is able to operate in a multi-network environment. The ability to share information across different networks will greatly enhance the usefulness of TwiddleNet in humanitarian aid and disaster relief operations.

TwiddleNet uses wireless IP-based architecture. Initial assessment is that there are no or only minor modifications required to the TwiddleNet application to allow it to interoperate with standard TCP/IP protocol for cross-network information sharing. As the Portal application manages the flow of information between all hosts, the key focus is to understand the Portal processes, to determine the changes required on the architecture that would allow hosts to send information across networks.

The Portal has three basic responsibilities within the TwiddleNet architecture [4]: (1) to store and process metadata (2) to service file request (3) to alert subscribers to any new content. The Portal application participates as a mid-tier in all communications between the content providers and the subscribers. When a content provider shares information, there are two possible scenarios [2] that could happen. They are: (1) Client serving: the content owner will provide the content to the requesting content subscribers. Portal will direct all requests to the mobile client who owns the content. (2) Portal

Caching: Portal will temporarily cache the content shared by the content owner. All downloading requests are served by the Portal instead of the mobile client who owns the content. In both cases, the Portal will have to uniquely identify both the content providers and subscribers. In another words, the Portal must be able to resolve the IP to a legitimate mobile client, regardless of which network the mobile client resides on.

THIS PAGE INTENTIONALLY LEFT BLANK

II. CURRENT ARCHITECTURE AND GAPS

A. TWIDDLENET ARCHITECTURE

The TwiddleNet system is comprised of three key components: Portal, Command Center and Clients. These three components are connected together in a Wireless Local Area Network (WLAN) via an Access Point as shown in Figure 1. The Portal and Command Center are statically deployed, and the clients are the only mobile components to be used at the area of operations. The clients are also the originators of the contents for sharing within the WLAN. When the TwiddleNet application is launched from a client, it will require the client to register with the Portal. The purpose is to allow the Portal to keep track of the clients in the network for receiving and forwarding of messages. The Command Center stores all the information sent from the clients and displays it in a Web page. The consolidated information in the Command Center can be used by the Commander for decision making. The detailed operation of each component is described in Figure 1.

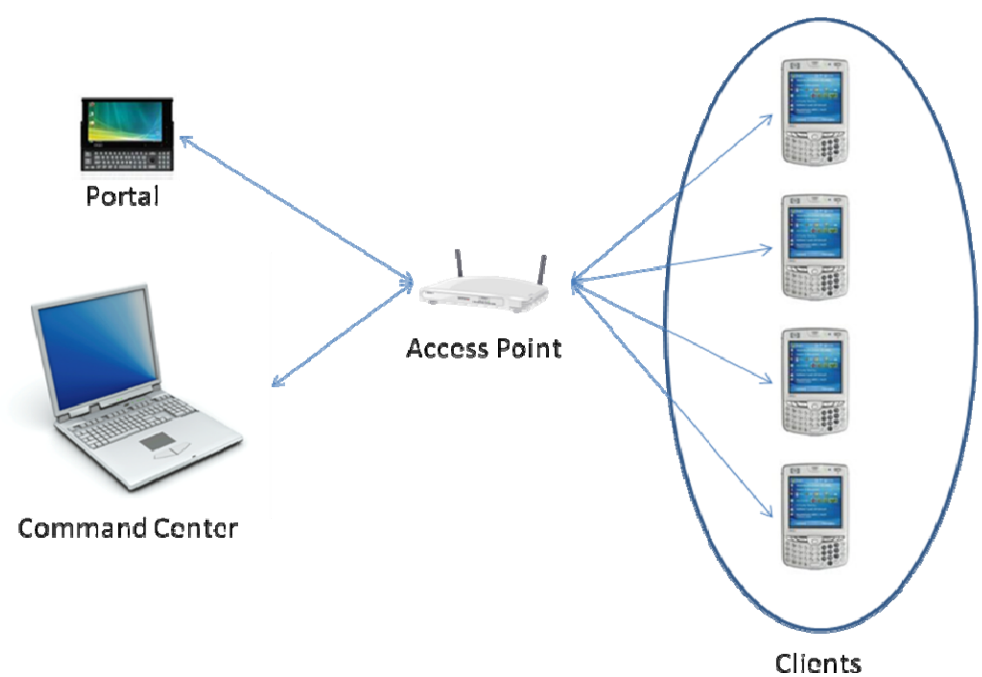

Figure 1. Overview of TwiddleNet Connectivity

1. Portal

The Portal is the heart of the TwiddleNet and should be the first component to set up. Without the Portal, the clients and the Command Center will not be able to function properly. The Portal has a database that stores the user account and passwords for authentication. It also keeps track of all the registered clients. Therefore, a user must first login to the Portal through the TwiddleNet application running on the client, in order to identify him as an authorized user. Upon successful login, the Portal will keep track of the IP address of the client. As such, the Portal will have a list of all the IP addresses of the clients that have registered to it. If a client has captured a picture for sharing, the Metadata of the picture will be sent to the Portal. The Portal will then forward the information to other clients, directing them to download the picture from the content provider.

2. Command Center

The Command Center is an integral part of the system for the Commander. It provides a collection of all the content sent by all the Clients for the Commander to make decision in an operation. It is also a service provider for authorized systems to connect to it to view the Command Center information. Similar to the Client, the Commander Center is also required to register with the Portal in order to receive information updates from the Clients. However, there is no need for man-in-the-loop to download the picture from the content provider. The application running at the Command Center will perform the downloading automatically. The pictures downloaded are then displayed on a webpage hosted at the Command Center. Subsequent downloaded pictures are then appended to the list of pictures in the webpage. The Command Center is also able to tag additional information to the picture received. However, this information is not sent out to the network and can only be viewed by authorized systems that access the Command Center.

3. Clients

The Clients are used by the users to capture and share information. In order to use the TwiddleNet application, clients need to be identified by an IP address. IP address can be obtained either by enquiring a DHCP server or by a static IP address configuration. During deployment, the system has the flexibility to connect itself to a DHCP Server from another Organization in the network. The system can also set up its own DHCP Server for its clients to connect to. In the lab set up, the Command Center is also a DHCP Server. Once the client has an IP address and has a link to the Portal, it can launch the TwiddleNet application. The application will first lead the user to logon to the Portal with a valid user account and password. Upon successful logon, the client IP address will be registered with the Portal. When a user captures a picture of an incident using the camera of the mobile device, the application will automatically send out the Metadata of the picture to the Portal. The Portal will then forward the information to other clients. When other clients received this information in a form of an alert message, they can download the picture from the originator directly.

B. GAPS

1. Range

The Portal, Command Center and Clients are connected via an Access Point. While specialized access points can provide a coverage of several hundreds of meters, a typical Access Point can support to a radius of 100m [6]. This means that Portal, Command Center and Clients have to operate at a radius no longer than 100m. In some cases, this may not be very practical. For example, Fireman may be divided into two teams to fight forest fire at two locations. The two locations are more than 200m apart and both teams are reporting to the same Command Center. Since the operating range of the Access Point cannot reach both locations at the same time, the two teams of Fireman are not able to share information. This constraint will restrict the practically of the use of TwiddleNet beyond the range of the Access Point. Content sharing within a 100m radius may not be meaningful as all teams share the similar views. Whatever all teams can see is also visible to the Command Center. As such, sharing of information to each other within a 100m range may not be necessary.

2. Cross Network Information Sharing

TwiddleNet is designed and tested on single network architecture. The transaction of message from one node[1] to another is within the same network. There is no requirement for the message to route from one network to another to reach and destination node and vice versa. In order to implement TwiddleNet on multiple networks, there is a need to perform study and conduct tests to verify cross network information sharing is possible. One possible way of implementing cross network information sharing is to implement Inter-WLAN connection as shown in Figure 2. If one team has to deploy beyond the range of TwiddleNet WLAN, the team can set up its own WLAN or connect to an existing remote WLAN. Then link the remote WLAN to the TwiddleNet WLAN through WAN or Internet. However, one constraint to this configuration is that all the clients at the remote WLAN must not have conflicting IP addresses with the TwiddleNet WLAN devices. The situation of conflicting IP addresses is likely to happen as Service Providers or agencies providing the WLAN are likely to use private IP addresses to manage their own network devices. There are chances that the IP addresses allocated to the clients at the remote WLAN are the same as the IP addresses allocated at the TwiddleNet WLAN. In this case, the concept of remote WLAN to extend the range of TwiddleNet will not work.

[1] Refer to Client, Command Center or Portal.

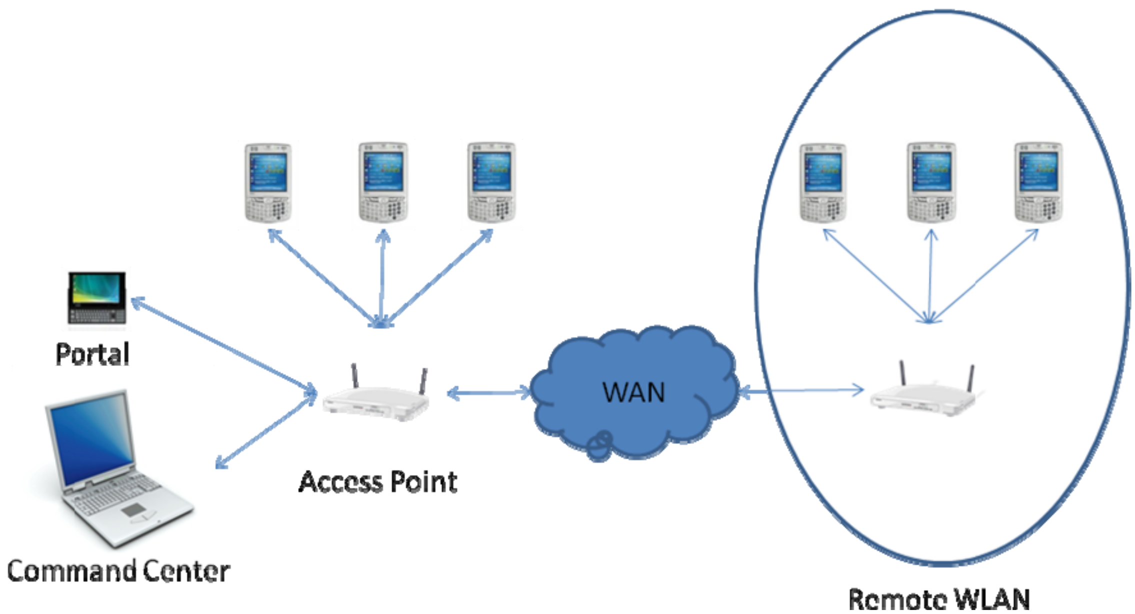

Figure 2. TwiddleNet Inter-WLAN Connectivity

THIS PAGE INTENTIONALLY LEFT BLANK

III. DESIGN CONSIDERATIONS FOR TWIDDLENET ARCHITECTURE TO ALLOW CROSS NETWORK INFORMATION SHARING

The purpose of the new architecture TwiddleNet design is to extend the capability to allow it to operate in more than one network. Such capability will enable the Response Team to operate in areas beyond the coverage of a single network. In fact, the Response Team should have the flexibility to operate in any network that has a linkage to the Command Center. As such, the design of TwiddleNet has to be carefully thought through so that the requirements can be met and yet the fundamental characteristics of the system will not be affected. The following are the general design considerations for the TwiddleNet:

A. PORTABILITY

One of the key benefits of TwiddleNet is that it is portable. It allows a small team to carry and deploy in area of operations easily without the need of heavy machinery or massive manpower. The overall size and weight of all the equipment is also small enough to be carried by many types of transportation. As such, any additional device added to TwiddleNet to allow cross-network information sharing should not affect its characteristics of portability. The overall size and weight of TwiddleNet should not increase significantly with the additional devices. Consequently, deployment considerations should remain the same for the new TwiddleNet architecture.

B. SIMPLICITY

TwiddleNet uses only a few portable devices for deployment. This allows the entire system to be set up easily, even by one person. Half-day training is also sufficient to allow a person to have the knowledge to deploy the system without guidance. This also implies that the transfer of knowledge for sustainability is simple. Therefore, the new architecture of TwiddleNet should not transform a simple system into a complex one. The system should continue to be simple to set up and configure. It should be easy to manage such that a person should not take more than 20 minutes to complete the entire set up. The system should also allow tests to be performed easily to verify for correctness. Finally, the new TwiddleNet architecture should require no steep learning curve in order to operate it.

C. FLEXIBILITY

The nature of each operation is different and the system should be able to configure accordingly to support each of them. The system should have the flexibility to configure with a standalone network or ride on an established network set up by another Organization. For example, the system may ride on the network established by the U.S. Navy in the area of operations for communication back to the Command Center. Alternatively, the system can be set up as a standalone network for communication if there is no other available network to ride on. As such, the system should have the flexibility to configure to work on the best available network infrastructure. In addition, the system should have the flexibility to configure to work on more than one network. The clients may be configured and distributed in separate networks and yet able to communicate with each other, and with Portal, as if they are sitting on the same network.

D. COMPATIBILITY

The next generation of TwiddleNet will be using the current version of TwiddleNet as a baseline to develop a subsystem for cross-network information sharing. The design of the subsystem must be compatible with the baseline, such that there should be no interoperability issues. The subsystem should use the same protocol as the baseline for message exchanges and a converter should not be required to perform the conversion of these messages. In addition, there should not be any proprietary application required to access the data in the Command Center. A remote terminal should be able to access the webpage hosted in the Command Center using a common browser such as Internet Explorer.

E. MAINTAINABILITY

TwiddleNet uses Commercial-Off-The-Shelf (COTS) devices, which do not require frequent maintenance. These devices can also be easily replaced by equivalent models from the commercial market. In addition, there is minimum caching in the application and it does not need regular housekeeping. The design of the next version of TwiddleNet will continue to take the same approach to reduce the risk of obsolescence by using hardware that is easily available and replaceable from the commercial market. In addition, the application will adopt minimum caching and configuration to minimize the need for housekeeping.

F. COST

TwiddleNet uses COTS hardware to build the system. This reduces the risk of obsolescence, as upgrades of the hardware are possible. Upgrading obsolete hardware is usually cheaper in the long run, compared to maintaining it. COTS hardware also has a lower maintenance cost as parts are more easily available. Moreover, COTS hardware is usually maintenance free. This means that there is no need to spend on regular maintenance to keep the system alive. Therefore, the life-cycle cost of TwiddleNet can be kept low. The next version of TwiddleNet will continue to leverage COTS for any additional devices.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. TESTS AND EVALUATIONS

A. TEST OBJECTIVE

The test objective is to evaluate the new architecture design of TwiddleNet that supports cross-network information sharing. Test setups are derived based on probable real-life scenarios and operations in disaster relief works. The testing will verify that the new design is able to overcome the constraints of the existing system to share information across networks. The testing will also verify that the design is able to function in a multi-network environment.

B. TEST SCENARIOS

Massive and multiple disasters have struck the central coast area. Monterey is chosen as the disaster relief headquarters due to the availability of power and communication network infrastructures. TwiddleNet is set up in the disaster relief headquarters, which is at least 30 miles away from the disaster sites. The first responders from various agencies are tasked to assess the severity of the situations at different locations. Only a basic network infrastructure is established at various disaster sites. The first responders, equipped with the TwiddleNet clients, are dispatched to different disaster sites. Numerous pictures of the frontline situations are captured and disseminated using those clients. Planning and resource prioritization are then based on the assessment of the real-time information shared. The system is configured as shown in Figure 3 to support this operation.

Under this scenario, the Command Center and Portal will be set up in a disaster relief headquarters. The headquarters is likely to be in a location where there are electrical power and network infrastructures. As such, the Command Center and Portal will be able to ride on this infrastructure to collect real-time contents from the TwiddleNet clients at various frontline sites. TwiddleNet clients will have to ride on the network infrastructure provided by the remote disaster site to communicate back to the

Command Center and Portal. The three possible ways of communicating from the remote disaster site to headquarters include Internet, satellite communication and radio communication.

Existing TwiddleNet is always set up under a single network. This means that the Command Center, Portal and clients are all sitting on the same network. This setup will not be very practical for the scenario described above. This is because the TwiddleNet devices can only operate within the range of a single network. If the capability of existing TwiddleNet is extended to operate in multiple networks, it must be able to operate under the IP address range provided for each network. As each network is likely to use private IP addresses, some form of Network Address Translation (NAT) must be used to allow TwiddleNet devices to communicate on different networks. A study of the TwiddleNet architecture suggests that COTS solutions can be explored to resolve such issues. In this thesis, there are two tests conducted for two types of setups for TwiddleNet under multi-network environments. The details of the tests are further illustrated below.

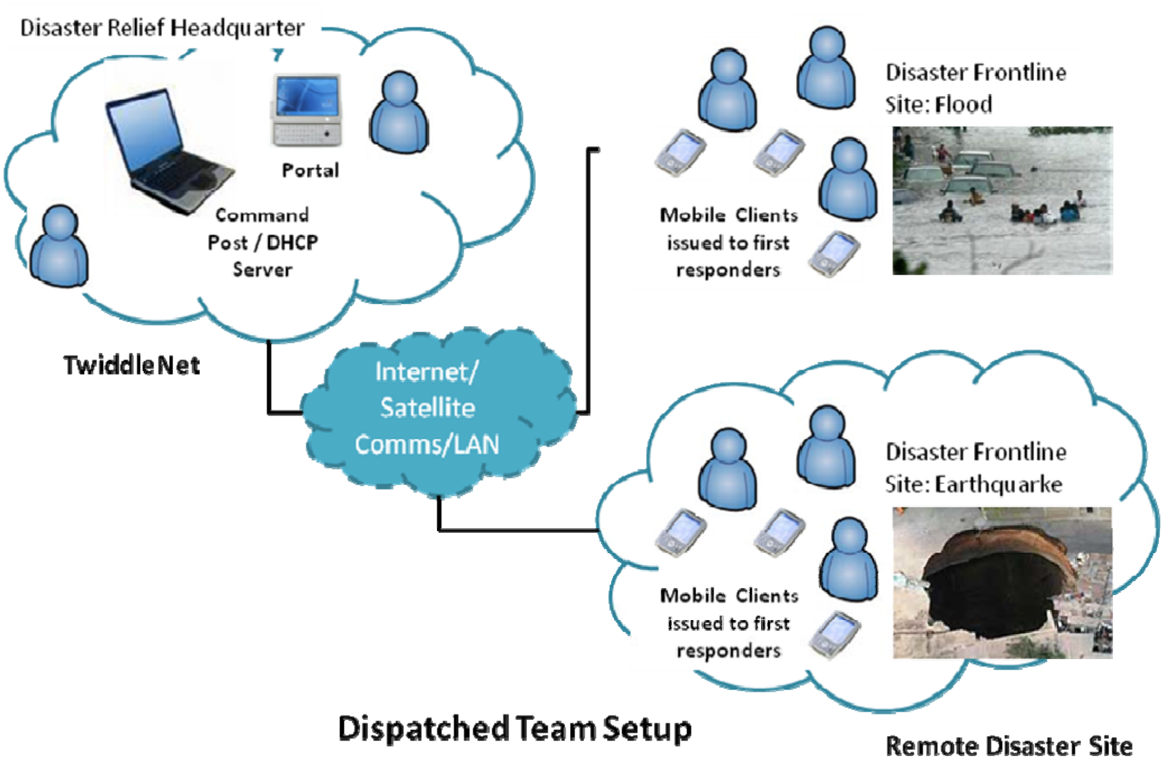

Figure 3. TwiddleNet Configuration to Support Disaster Relief Operations

1. Distributed Setup A

In this setup, it is assumed that local site (Subnet A) and remote site (Subnet B) are managed by either a single agency or coordinated agencies. This is because the devices in both sites are configured with unique IP addresses. The Dynamic Host Configuration Protocol (DHCP) server in each subnet is used to allocate IP addresses to devices for each site. The two DHCP servers do not allocate conflicting IP addresses and there is no need for network address translation. Figure 3 is an illustration of this setup. The purpose for this setup is to verify that cross-network information sharing is achievable by configuring a few additional COTS hardware items into the system. The configuration uses two wireless access points for two Wireless LANs (WLANs). The two WLANs are then connected using a router.

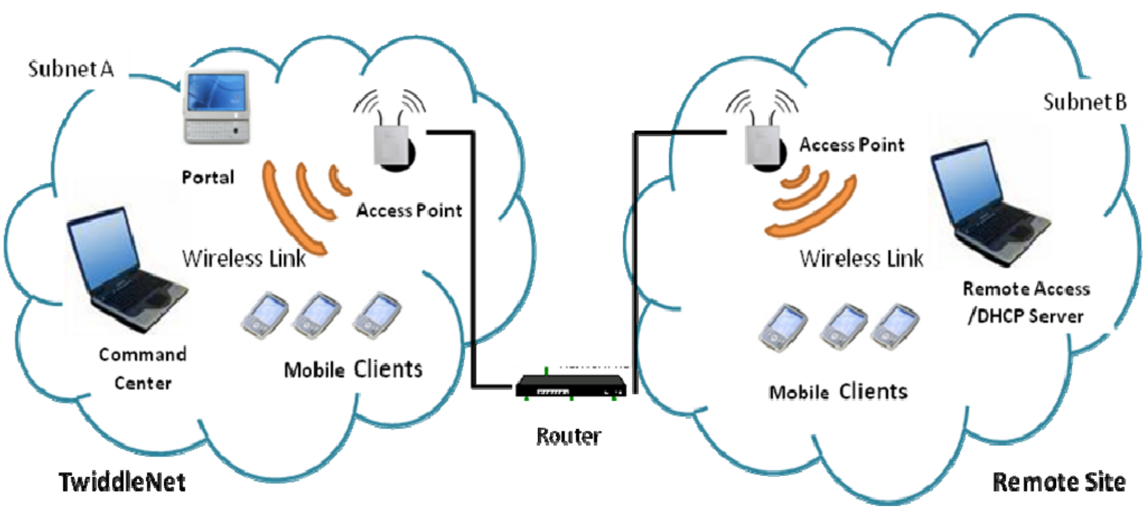

Figure 4. Distributed Setup A

a. Configuration

Subnet A is configured to represent the setup of TwiddleNet in a disaster relief headquarters. The setup is comprised of the Command Center, Portal and a few mobile clients. Subnet B is configured to represent the deployment of the TwiddleNet clients at a remote site. The setup assumed that the network infrastructure at the remote site is readily available, and that a link is established between headquarters and the remote site. This link is simulated in the lab by wiring two access points together through a router. The IP addresses for the clients are allocated by the DHCP server at each site. The table below shows the IP addresses allocation for the setup.

Devices	IP
SubnetA	**192.168.1.0/27**
Router Interface	192.168.1.254/27
Access Point	192.168.1.1/27
Command Post	192.168.1.4/27
Portal	192.168.1.3/27
Mobile Clients	192.168.1.11/27 – 192.168.1.20/27
Subnet B	**10.0.0.0/8**
Router Interface	10.215.175.33/8
Access Point	10.215.175.34/8
DHCP Server	10.215.175.35/8
Mobile Clients	10.215.175.80 to 10.215.175.90/8

Table 1. IP Addresses Allocation for Distributed Setup A

b. Evaluation

In the test, the process of clients signing on to the Portal and sharing of information is exactly the same as the process for single network. The test shows that the clients from both subnets are able to logon to the Portal. Clients from Subnet A are able to share information to clients at Subnet B and vice versa. The Command Center is also able to receive the information from all the clients. Under this setup, every TwiddleNet device is required to have a unique IP address. However, this might not be possible in reality.

The reason is that there might not have enough IP addresses for all the devices that are deployed for the operation. It is also very difficult to manage a large range of IP addresses and to ensure that no two devices will end up using the same IP address. To resolve this problem and to minimize the impact on the existing network infrastructure, each subnet can form a private network with a gateway to interface with other subnets. Distributed Setup B is an illustration of such configuration.

2. Distributed Setup B

This configuration uses three subnets. Command Center and Portal are operating in Subnet A. TwiddleNet clients are operating in both Subnet B and C. All the TwiddleNet devices are using private IP addresses. This means that TwiddleNet device in Subnet A can have the same IP address as TwiddleNet devices in Subnet B and C. This situation is possible as subnets may be managed by different agencies and each subnet may not have enough public IP addresses for all the devices. However, current TwiddleNet system does not allow devices to have conflict IP addresses. As the Portal need to be able to resolve the IP address and send the messages to the correct clients. The new TwiddleNet design provides the flexibility for devices to use common IP addresses by using gateways. The primary role of gateways is to perform network address translation for the hosts sitting in the private network. In this way, devices in all the subnets are able to communicate with each other regardless of whether they are private IP addresses.

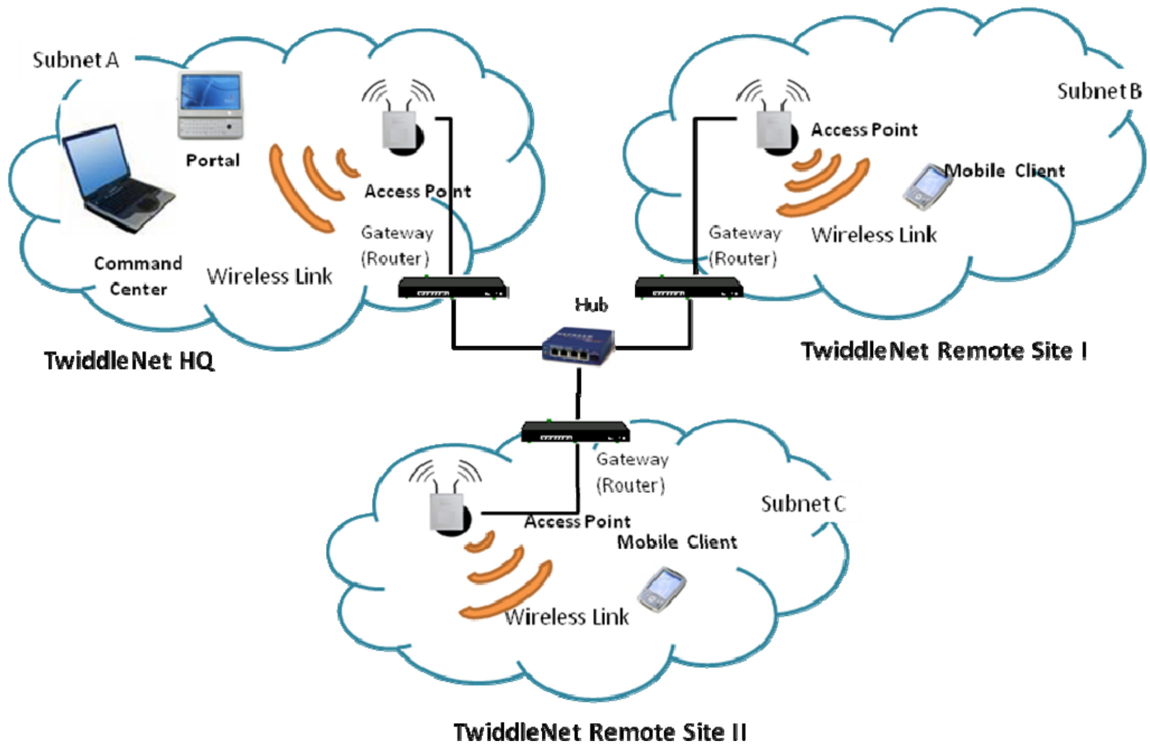

Figure 5. Distributed Setup B

a. Configuration

The test setup includes three private networks namely TwiddleNet HQ (Subnet A), Remote TwiddleNet I (Subnet B), Remote TwiddleNet II (Subnet C). All networks are interconnected via a Hub.

Devices	IP	Translated IP
SubnetA	**192.168.1.0/27**	
Router Interface	192.168.1.254/27;10.215.275.33/8	
Access Point	192.168.1.1/27	
Command Center	192.168.1.4/27	
Portal	192.168.1.3/27	10.215.175.3/8
Subnet B	**192.168.1.0/27**	
Router Interface	192.168.1.49/27;10.215.175.37/8	
Access Point	192.168.1.50/27	
Mobile Client	192.168.1.11/27	10.215.175.41/8
Subnet C	**192.168.1.0/27**	
Router Interface	192.168.1.100/27; 10.215.175.100/8	
Access Point	192.168.1.51/27	
Mobile Client	192.168.1.11/27	10.215.175.101/8

Table 2. IP Addresses Allocation for Distributed Setup B

b. Evaluation

With the implementation of the three gateways, all Subnet A, B and C hosts are able to communicate even they are sharing the same IP space. All private IP addresses are translated into unique IP addresses as shown in Table 2. Content sharing between the command post in Subnet A and the mobile clients residing in Subnet B and Subnet C is achieved successful without any issue. Clients in Subnet B and C are able to share information with each other although they have the same IP address. This is made possible through the implementation of gateway.

3. TwiddleNet Field Trial

The TWIDDLENT field trial was conducted during the Tactical Network Topology (TNT) Evaluation from 17 November 2009 to 18 November 2009 at Camp Roberts. The TNT architecture set up at Camp Roberts consisted of three wireless networks interconnected by tactical radio link as shown in Figure 6. This provided a good environment to test the new TwiddleNet architecture design for cross network information sharing. As the tactical radios are able to support data communication between two nodes that are located several kilometers apart, the tests would also show that the TwiddleNet is able to operate beyond the range of a single network. During this trial, tests were conducted for two types of setup to evaluate the performance of TwiddleNet data communication through the tactical radio. The details of the trial can be found in ANNEX B: TwiddleNet Onsite Trial.

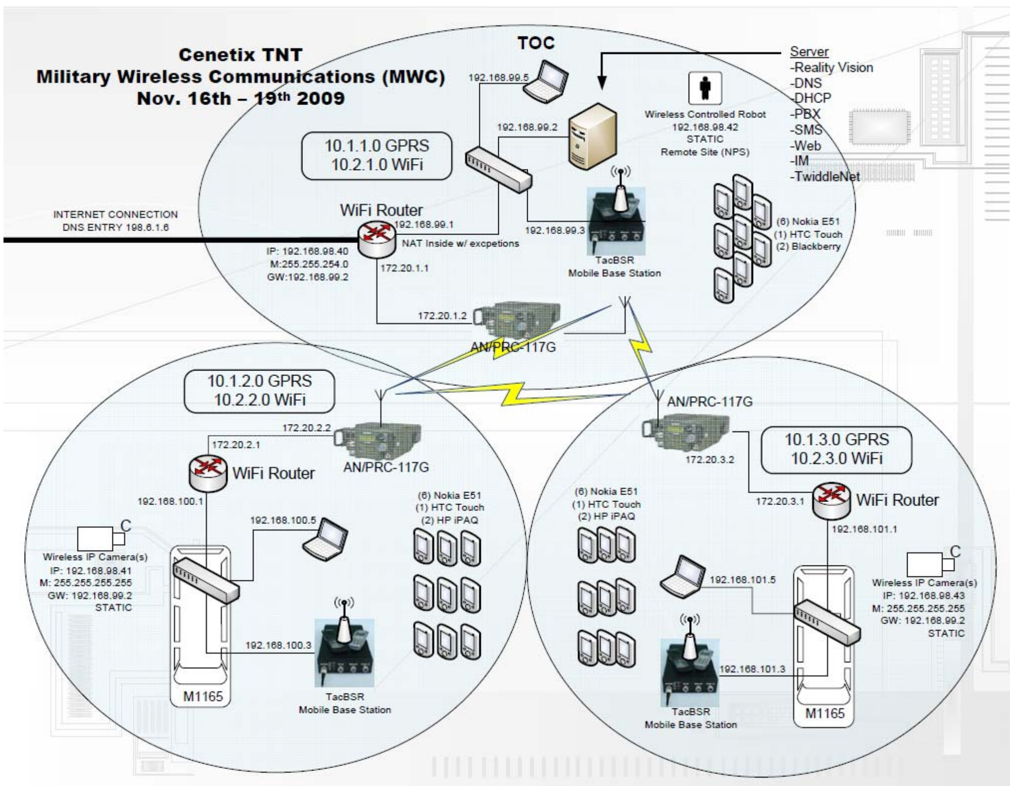

Figure 6. TNT Network Diagram [3]

a. Setup A

Command Center, Portal and mobile client B were connected to Subnet Area 1 for this setup. Only Mobile client A is connected to Subnet Area 3. Under this configuration, client B was able to communicate directly with Command Center and Portal through the same Access Point. However, client A would need to need to go through the TNT radio link to reach the other TwiddleNet devices in Subnet Area 1. In this test, one picture was taken by client A at one-minute intervals for a total of ten pictures. Measurement was then recorded to note the time taken for each of the message to reach client B. The result shows that it took 4 to 9 seconds for the alert message to reach client B and it took an average of 3.3 seconds for client B to download picture from client A.

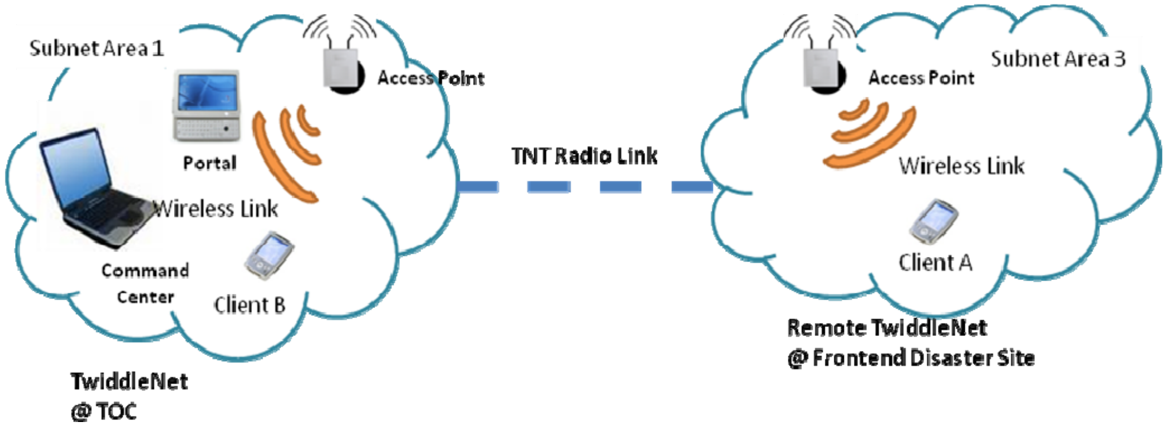

Figure 7. Network Diagram for Setup A

b. Setup B

In this setup, only the Command Center and Portal were connected to Subnet Area 1. Both client A and B were connected to Subnet Area 3. The purpose of this test is to verify that the message sends from client A is able to reach Portal through the radio link and client B is able to receive the alert message from Portal through the same radio link. The same procedure from Setup A was used in this setup. One picture was taken by client A at one-minute intervals for a total of ten pictures. The result shows that it took 3 to 8 seconds for the alert message to reach client B, and it took an average of 1.5 seconds for client B to download picture from client A. It can be observed that the time taken for client B to download picture from client A is much faster in Setup B. This was because client B was able to access client A from the same Access Point.

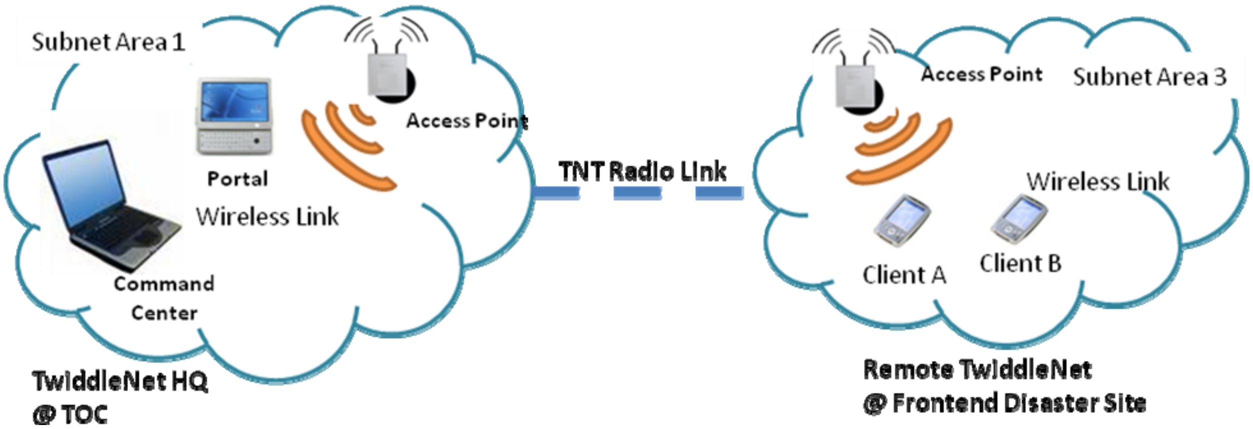

Figure 8. Network Diagram for Setup B

V. POSSIBLE ARCHITECTURE FOR FUTURE GENERATION OF TWIDDLENET

A. CONSTRAINTS ON CURRENT ARCHITECTURE

Connectivity is an essential part of the TwiddleNet. The system requires a stable connection throughout the operation of the system. The process of the information sharing will be affected if any device is unable to connect to the network. The requirement of having all devices to be connected to network at all time is challenging when deploying TwiddleNet in the field. This is because there are many factors that can affect the connectivity in the field environment. With this as the background, the following material describes the challenges when using TwiddleNet.

1. Launching of Client Application

In order to use the application on the client, the client has to establish a connection to the system. Firstly, it has to be connected to a WLAN and obtain an IP address from a DHCP Server or configure with a static IP address manually. Secondly, there is a need to make sure that the Portal is connected to the network and the applications on the Portal are running. Lastly, the client will need to login to the Portal with a User ID and password. Upon successful login, the client application will be able to launch. This process shows that there must be an established connection between client and Portal in order to launch the client application. Ensuring that client and Portal are connected through a single network is easy, as the client and the Portal are collocated at the same site. For a multiple networks connection, where client and Portal are located hundred miles apart, it may not be so easy . Good coordination and good support between sites is necessary to make sure the connection between client and Portal is established.

2. Using of Client Application

The client application requires access to the Portal through the WLAN connection to perform tasks such as sharing items, un-sharing items and downloading items. If the network is not available or the Portal is not reachable, some of the tasks will not be performed properly by the application. In some cases, this may result in the need to launch and log in to the application again. As such, the application is highly dependent on the availability of the network and the Portal. Therefore, it is necessary to ensure a stable connection from client to Portal when using the application.

3. Sharing of Information

The clients sharing the information do not know the present of other clients and do not check if they have received the information. As such, it is likely that not all the clients will have synchronized pictures. The receiving clients also do not know if the information they have in the database is the latest, as they do not know if there are updates that they failed to receive. For the client to resend the information, it has to search for the image in the folder and add it to the Shared List in the application for sharing out to other clients. However, the application is unable to selectively choose a particular client to send the information to. It can only send the information to a group of clients, regardless of whether some of the clients have already received the information previously. As such, a resend action may result in some clients receiving duplicated information.

4. Creation of Contents

The application has a fixed format for creating information for sharing. There is no flexibility for the clients to create the contents of the information before sending it out. If a fireman captures a picture of the fire situation using a smartphone, he does not have the flexibility to insert information about the fire through the application, other than the tagging mechanism supported by the system. As such, the information provided by the content provider may not be sufficient for the Command Center to make a good assessment. In addition, the resolution of the pictures taken by a smartphone may be lower than desired. Without further information, a photo may not make sense to the Commander. If there is flexibility to insert an additional description with the picture, it will provide meaning to the information being sharing.

B. MOBILE WEB SERVER (MWS) CONCEPT

1. Operating Concept

The concept of MWS uses mobile devices such as smartphones to host information and function as a Web Server. A computer can then access the information from the mobile device by using a browser. The architecture of the MWS has three key components: the Browser, the Mobile Device and the Gateway, as shown in Figure 9. The Gateway relays messages between Mobile Device and Browser such that virtually the Browser and Mobile Device are connected directly. To begin the operation, the Mobile Device has to register itself to the Gateway, so that the Gateway is able to know the current IP address of the Mobile Device and able to route the requests from the Browser to the correct Mobile Device. This means that each Mobile Device operating as a MWS must have a unique IP address to register to the Gateway. When someone enters the URL to the MWS, the request is forwarded to the Gateway after the DNS resolution. The Gateway then inspects the HTTP request header to identify and forward request to the correct MWS. In a similar way, the reply from the MWS is sent to Browser through Gateway [7].

Figure 9. Key Components of MWS

2. Strengths of MWS Architecture Compared to TwiddleNet

a. Launching of Application is Straight Forward

The application does not depend on the presence of a network or other devices. This is because the client is a Web Server, and a user can launch the application without the need to establish a link. This is crucial to first responders, as critical information might need to be captured prior to any form of linkage can be established. For example, the medical team might need to start using the application to capture the information on casualties upon arrival at the site, before a network is established, so that the information can be made available to the Command Center for decision making once the network connection is up.

b. Use of Application is Independent of the Network

The process of using the application, from beginning to completion, only happens on the client. There is no involvement of other devices or subsystems. As such, the application is not constrained to the availability of other devices or subsystems. This is an important feature for the first responders who are going into a disaster site. The first responders are likely to be the first to enter the disaster site, and there is no infrastructure to allow them to have a stable data link to the Command Center or Portal. It is not likely that the first responders can afford to wait for a network infrastructure to be established in order to perform their duty. The MWS allows them to start capturing information even without a network. When the network is available later, the information captured can be shared to the Command Centre immediately. This feature also allows someone to enter a site that has no network infrastructure to capture information using MWS. When he returns to the base, or somewhere he can find a network connection, he can start sharing the information. Figure 10 illustrates this process of information sharing.

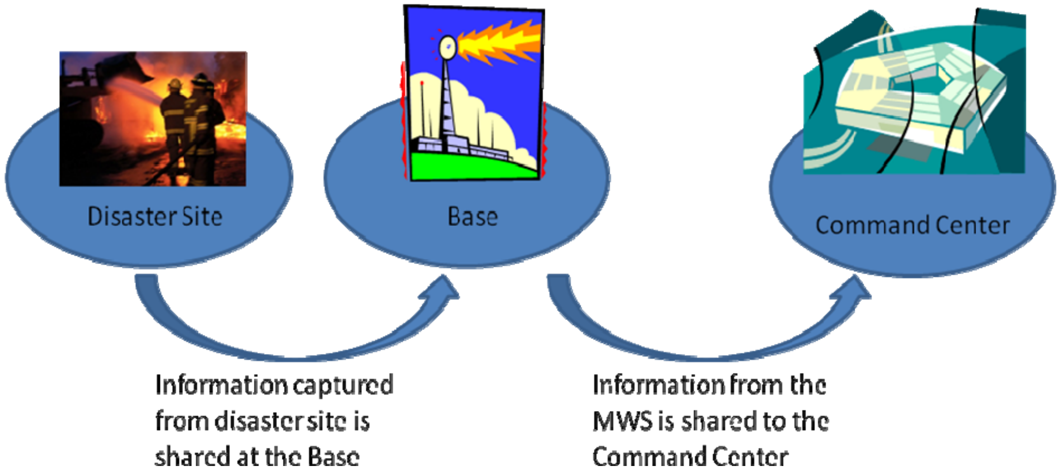

Figure 10. Process of Information Sharing for Site without Network

c. *Sharing of Information is Simple*

In TwiddleNet, one client cannot request information from another client through the application. There is a need to communication with the user of the other client using another communication means (e.g., voice channel) to request for information. For MWS, a client can request information from another client by entering the Uniform Resource Locator (URL). There is no need for the user of the other client to be in the loop to share the information. In this process, the information that is received will always be the latest from the contents provider. As such, there is no risk of making decisions with outdated information. Any client can always request updated information from any other client at anytime. Unlike TwiddleNet, other systems can also access to the clients for information, instead of just the Command Center.

d. *Creation of Contents is Flexible*

Every mobile device running MWS is functioning as a Web Server, and every user is an administrator to his mobile device. The user has the administrative rights to put in or take out data from the Web page. He is not restricted by the format of the contents he wishes to share. This is an important feature for the first responders in some situations, and the formatted messages are not sufficient to represent certain important information. For example, a fireman may want to share information about the condition of the forest fire and the direction that the fire is spreading. This can be a piece of important information to his fellow firefighters working in that direction. This information is also important to the Command Center for making decisions to send reinforcements to the right location. When information is limited to pictures alone, the information is insufficient.

3. Shortcomings of MWS

Since every client running as MWS is a Web Server, the information is contained inside the client. If client B had access to client A before,, it has to access client A again if it has to view the information again. This is similar to access NPS's Web Server to view the homepage. One must access NPS's Web Server again, if there is a need to see the homepage again. However, an MWS uses a mobile device and does not have the same capability as a normal Server. If all the other mobile devices are accessing the same mobile device, this mobile device may be too overwhelmed to handle the load. Even if the mobile device is able to handle the load, its battery life will be shorter as it has to perform more transmission tasks to reply to the requests. Another shortcoming of the MWS is that there is no application that reads and combines information from all the mobile devices into a page of information. A user will have to access each one of them, one at a time, to see the full picture. This may not be a problem if there are only a few mobile devices deployed, however, it can be a very tedious task to continue accessing ten, twenty, or more of such devices. Finally, the MWS does not have a feature to cache information that was last accessed. If a particular mobile device becomes unavailable, its past data will not be available for referencing in another location.

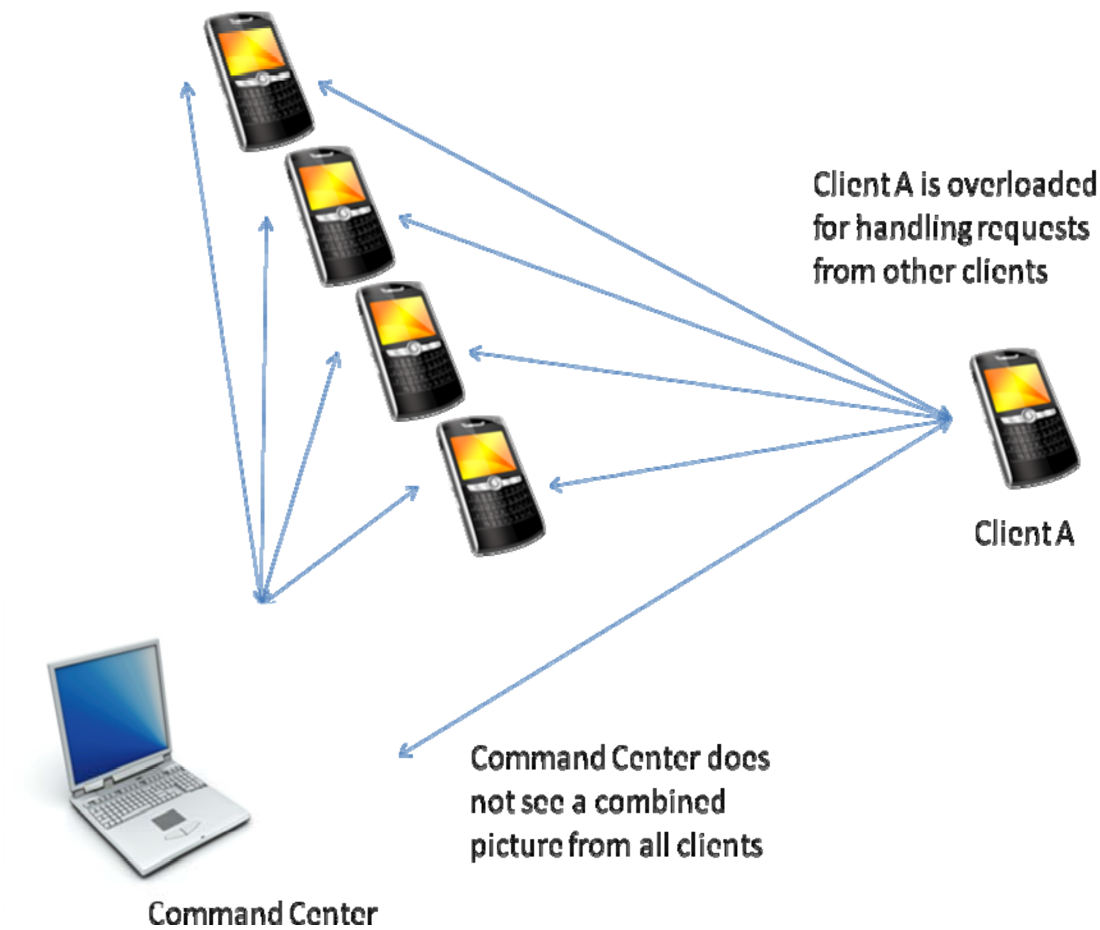

Figure 11. Shortcomings of MWS

C. TWIDDLENET ARCHITECTURE USING MOBILE WEB SERVER

There are many good features in MWS architecture that TwiddleNet can use to overcome some of its shortcomings. A Proposed Architecture of TwiddleNet is as shown in the figure below. There are three key components in this architecture: the Command Center, Gateway and TwiddleNet Clients. The functions of each component are described below.

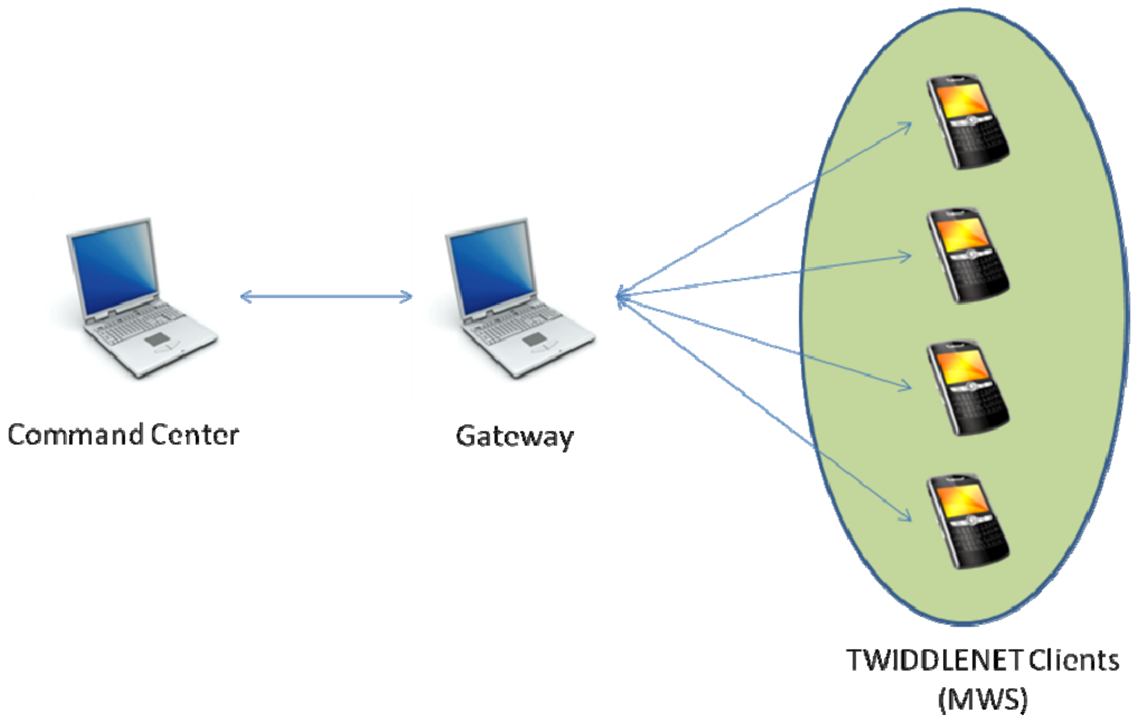

Figure 12. TwiddleNet Architecture using MWS

1. Command Center

a. Combine Clients' Information into a Single Web Page

The Command Center has a service that organizes all the information collected from the clients into a single page view as shown in the figure below. The Service keeps track of the updates from each client and then updates the respective column and row on the webpage accordingly. The Command Center serves the Commander with a comprehensive picture for decision making. At the same time, it also serves other systems, and TwiddleNet clients, as a web server. A client is able to selectively choose to see any other client information from the Command Center. For example, client B is unable to access client A directly. It can then choose to access the Command Center for client A's information instead, since the Command Center keeps an updated copy of information from client A. If only client A's information is requested from the Command Center, only client A's information will be provided to client B. This is to make sure that the bandwidth of the network is better utilized.

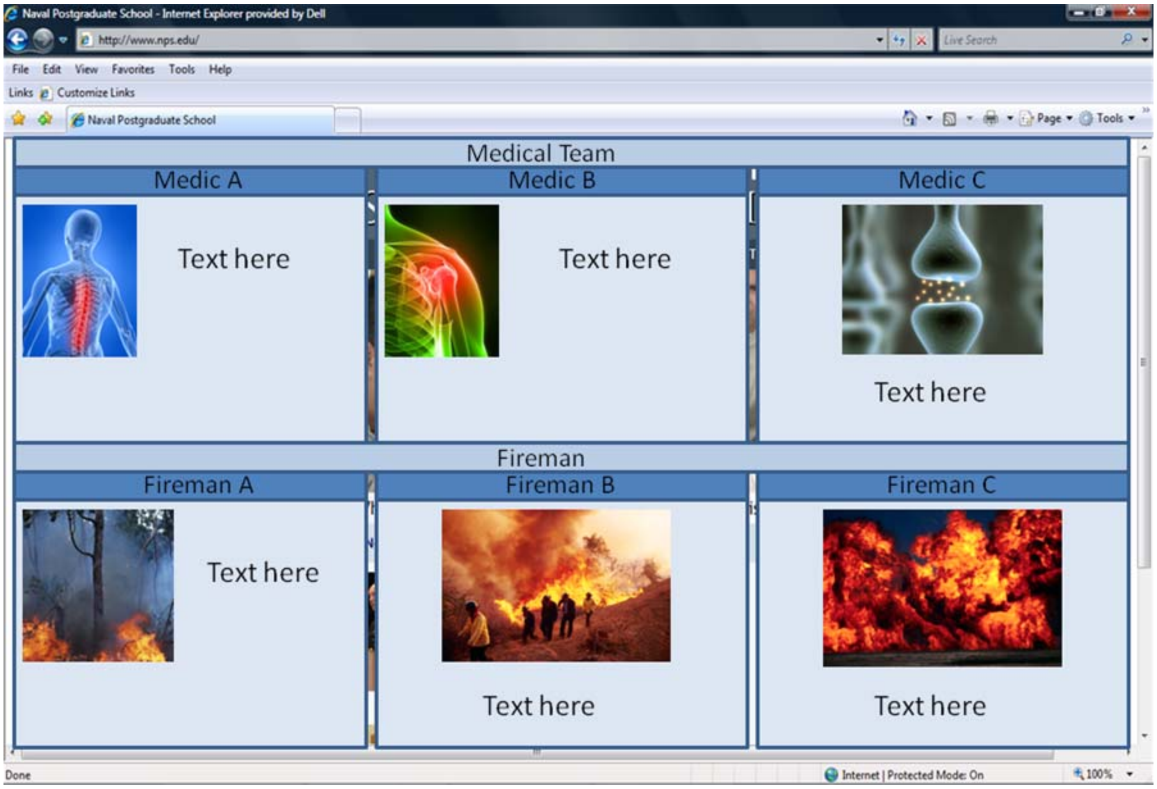

Figure 13. Webpage of Command Center

b. *Caching of Clients' Information*

The Command Center has a service that caches the information from the clients. This is to prevent unnecessary overloading of the network and the clients by minimizing constant access to clients. It also serves as a redundancy to the clients in the event that they became unavailable or overloaded. The service from the Command Center will pull the information for the client when it receives an update message from that client. This is similar to receiving an alert message in TwiddleNet. After the service pulls the information from the client, it stores it in the database and updates the webpage accordingly. The service also has the option to poll the information from each client at an interval such that it will not overload the network or the clients.

2. Gateway

The Gateway operates the same way as the gateway in the MWS. It relays the messages between a Requester and a Sender. When each client is connected to a network, it has to register its IP address with the Gateway; when client A enters the URL to client B, the Gateway will be able to resolve the IP address of client B and relay the messages between client A and B. The Gateway also keeps track of the active and inactive clients, such that if there is a request sent to an inactive client, the Gateway will be able to respond to the Requester immediately, instead of searching and waiting for timeout before informing the Requester that the client is inactive.

3. TwiddleNet Clients

a. Information Owner

The application on the client is able to generate information onto a webpage, using a template to minimize the steps required to share the piece of information. The application also has the flexibility to allow specific information to be updated into the webpage to make it more meaningful. When the webpage is first created or subsequently updated, a broadcast message will be sent to the network. The Command Center and other clients that receive this message will request the information from the information owner. The process of information sharing is as shown in the figure below.

b. Information Requester

When a client receives a broadcast message from another client informing of an update of information, it can choose to access the information if it is available. The client should have a caching capability such that the accessed information is stored locally for subsequent reference. The client should also have the option to request information from either the Command Center or the information owner (another client). In this way, neither the Command Center nor the information owner will become a bottleneck or single point of failure. By default, the client requesting information should access the Command Center so that it will not overload and drain the battery of the information owner. If the Command Center is not available, it can then access the information owner directly. As such, the Command Center and Information Owner will serve as redundancies to each other.

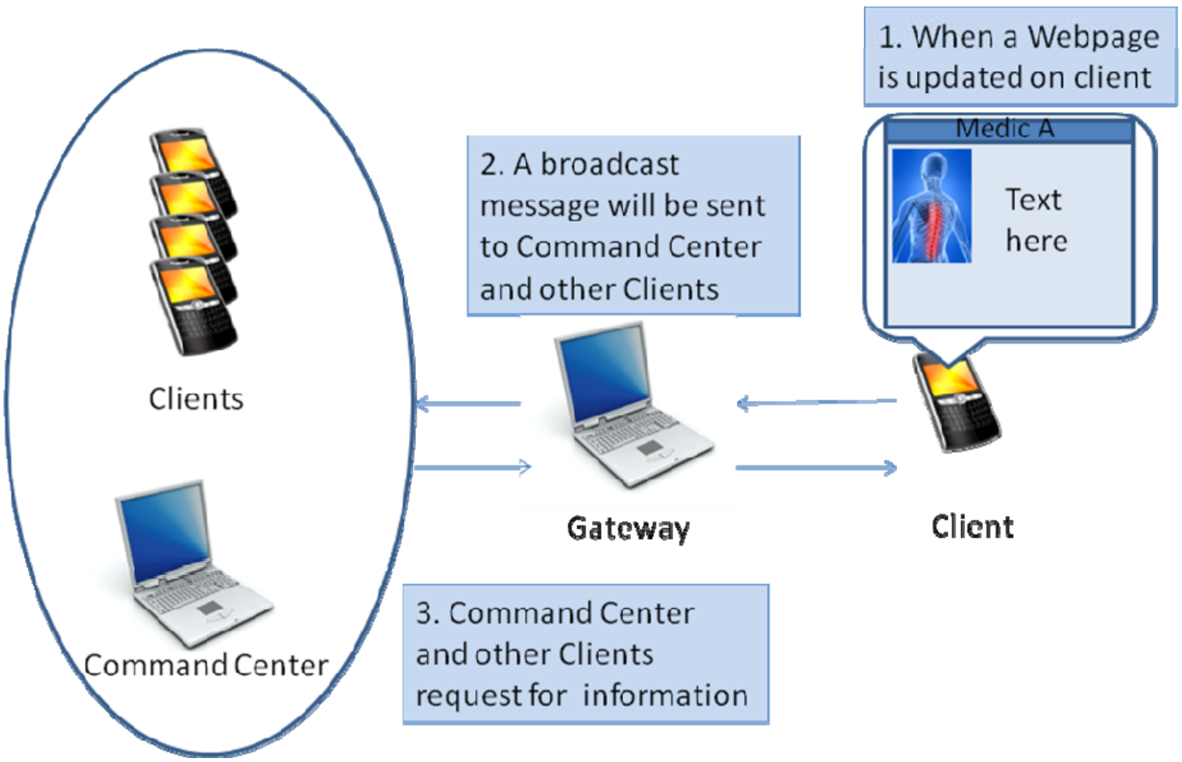

Figure 14. Process of Information Sharing

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS

TwiddleNet is an excellent system for first responders who are supporting humanitarian aid and disaster relief operations. It is portable and can be deployed quickly. The mobile client is also a very handy tool for the first responder to capture and share information to the Command Center in near real time.

On the other hand, the architecture of TwiddleNet is designed and tested to operate on a single network, which limits its range of operation to that of the network. Thus, it will be inadequate for the system to support large events, such as the occurrence of a major disaster.

Typically, multiple sites will be deployed when there is an operation that spans a large area. A network can be set up at each site to support the systems operating there. Each individual network can then be connected through the Internet, Satellite Communication or Radio Communication. The thesis is based on this idea of a multiple-network deployment in designing TwiddleNet to function in a multi-network environment. Tests were conducted in the lab and in the TNT field trial. The results show that the new TWIDDLENT architecture is able to support multiple networks; hence its range is no longer constrained to that of a single network. Instead, it is extended to the coverage of the Satellite Communication or the range of the Radio Communication. This is a significant improvement to TwiddleNet capability. TwiddleNet is now able to be deployed effectively to support humanitarian aid and disaster relief operations. With this extended capability, TWIDDLENT can potentially be used to support Hot War and Operations-Other-Than-War. It can be used to collect intelligence pictures and own force situation pictures at near real time.

The thesis also conducted a study of the Nokia Mobile Web Server to propose a new architecture of TwiddleNet. The MWS uses mobile devices to operate as a Web Server. Such a design allows mobile devices to run applications in the absence of network connectivity. In the case of TwiddleNet, no application can be launched without network connectivity. The drawback of the MWS is that it does not have a Command

Center that consolidates the shared information from all the clients into a single webpage. This study combined the strengths from both the MWS and TwiddleNet, and proposed an architecture for the next generation of TwiddleNet.

The capability of TwiddleNet in performing cross network information sharing had been demonstrated in lab and field trial. It is suggested to conduct tests involving actual users during field exercises to verify the performance of the system, so that the system may be used for operations in future. It is also suggested to develop a prototype using MWS to verify the new architecture for next generation of TwiddleNet. This new architecture is expected to improve the flexibility, efficiency and redundancy of information sharing.

APPENDIX A – VARIOUS TWIDDLENET COMPONENTS' ROLES

Portal

The primary function of the Portal is to serve as a gateway to a network of mobile clients. A central repository of metadata that describes the shared content is housed in the Portal. The Portal tracks and stores all IP information of the currently signed-in clients as well.

Command Post

A Command Post is a modified TwiddleNet mobile client that acts as a situational awareness tool. It is capable of downloading and displaying shared contents from any mobile client.

Lab LAN

Lab LAN includes a router that is configured to route IP traffic between two Subnets.

Access point

Each Subnet will incorporate an access point to provide wireless access for all wireless Subnet devices.

DHCP Servers

IP address management and allocation are done by DHCP servers.

Mobile Clients

TwiddleNet mobile clients can come from different groups, namely medics, firefighters and police. At least one client is included in each Subnet. Content sharing is then tested between mobile clients residing in different networks.

TwiddleNet Gateway

The gateway's primary role is to provide Network Address Translation for the TwiddleNet Private Network clients. Static NAT is implemented in DTS-B.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B – TWIDDLENET ONSITE TRIAL

A. INTRODUCTION

TwiddleNet is a hardware/software suite designed for use by agencies assisting in recovery efforts after a natural disaster or an emergency of any sort. Its main purpose is to quickly and automatically provide content sharing of pictures of important aspects of recovery efforts, to all users logged on to the TwiddleNet system, through the use of smart phones, a Portal and a Command Center. The majority of previous tests involving TwiddleNet have centered around operating the architecture on one network/subnet, and in this regard, the application runs very effectively. Operating in this manner could, however, in certain situations, limit the effective distance that users can be from one another, as one wireless network will not usually cover an entire area, organizations would have to be separated in their recovery efforts. To address this potential limitation, tests involving operating on more than one wireless network are necessary to solidify the utility of TwiddleNet

B. OBJECTIVE

As stated, prior testing with TwiddleNet has centered on operating on only one network, which will, in all likelihood, be insufficient in a real world rescue situation. The tested ability to operate on more than one wireless network would greatly enhance the utility of TwiddleNet in real world situations. The architecture set up at Camp Roberts, utilizing three wireless networks interconnected by tactical radio, provided the perfect opportunity to test TwiddleNet in this manner. The range of the tactical radios, several kilometers, would effectively extend the operating range of TwiddleNet to the same range, and the tested objective of our experiment is for a mobile device on one of the three wireless networks to pass data (pictures) through the gateway to the Command Center on another wireless network, and subsequently on to a different mobile device on a third wireless network.

C. RESULTS

1. Test Case 1

This test case has a Command Center, Portal and mobile client B connected to Subnet Area 1. Only Mobile client A is connected to Subnet Area 3. The configuration is as shown in Figure 1. The purpose of this test case is to verify that pictures captured and sent from a mobile client in the subnet are received by the mobile Client and Command Center on the other subnet. This test will require mobile client A to capture and send pictures across the TNT network at one minute intervals for a total of ten pictures. The measurement taken for this test case is shown in Table 1.

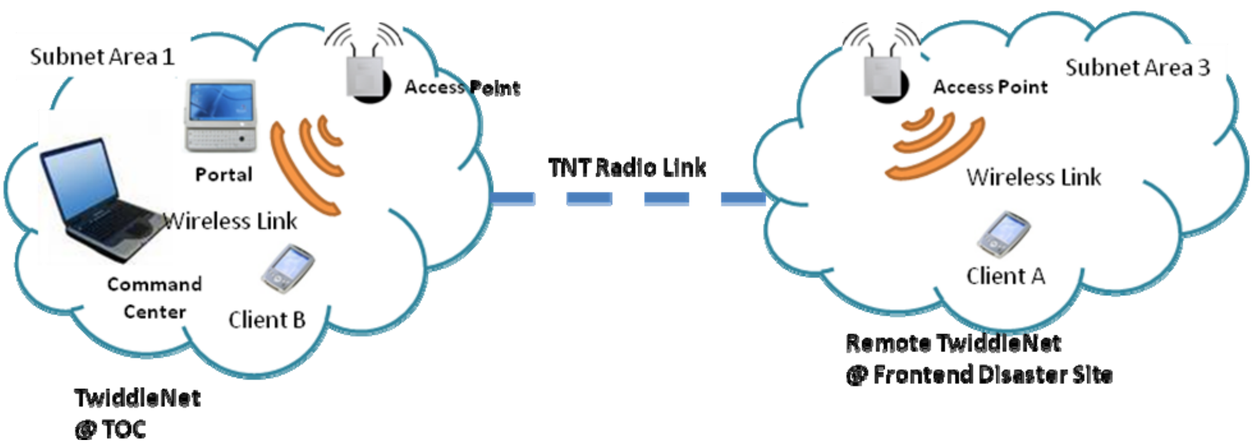

Figure 1: Configuration for Test Case 1

Pic. No.	Subnet Area1				Does the Command Center receive and post the picture on the webpage? (Yes/No)
	Does the Client receive the alert message? (Yes/No)	Time Taken for Client to receive message (seconds)	Is the Client able to download the picture successfully? (Yes/No)	Time Taken for Client to download picture (seconds)	
1	Yes	9	Yes	3	Yes
2	Yes	4	Yes	3	Yes
3	Yes	4	Yes	4	Yes
4	Yes	4	Yes	3	Yes
5	Yes	5	Yes	3	Yes
6	Yes	5	Yes	3	Yes
7	Yes	5	Yes	4	Yes
8	Yes	4	Yes	3	Yes
9	Yes	5	Yes	3	Yes
10	Yes	5	Yes	4	Yes

Table 1: Measurement for Test Case 1

2. Test Case 2

In this test case, only the Command Center and Portal were connected to Subnet Area 1. Both mobile clients A and B were connected to Subnet Area 3. The purpose of this test is to verify that the messages sent from mobile client A reach the Portal through the radio link and mobile client B is able to receive the alert message from the Portal through the same radio link. The same procedure used in Test Case 1 was used in this test. One picture was taken by client A at one minute intervals for a total of ten pictures. The measurements taken for this test case are as shown in Table 2.

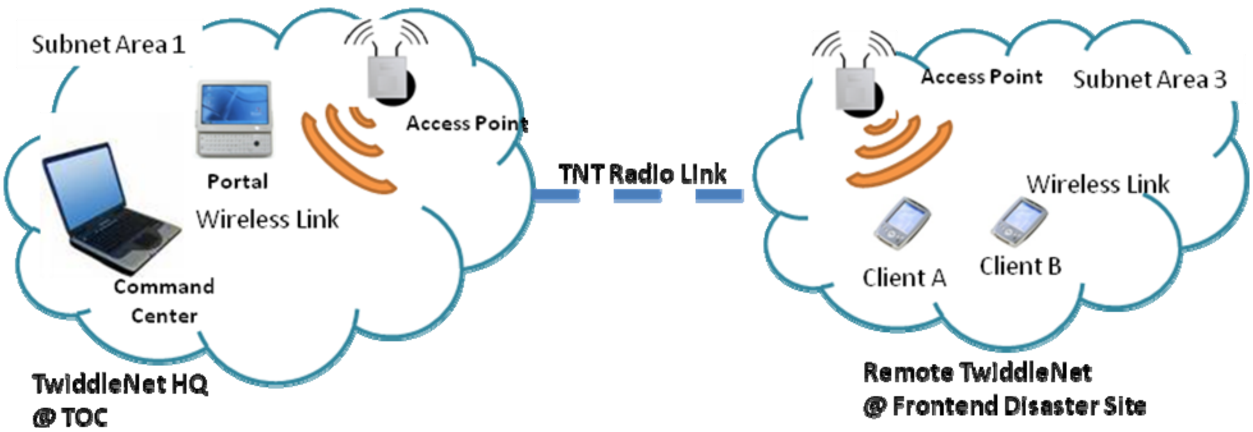

Figure 2: Configuration for Test Case 2

Pic. No.	Subnet Area3				Does the Command Center receive and post the picture on the webpage? (Yes/No)
	Does the Client receive the alert message? (Yes/No)	Time Taken for Client to receive message (seconds)	Is the Client able to download the picture successfully? (Yes/No)	Time Taken for Client to download picture (seconds)	
1	Yes	8	Yes	2	Yes
2	Yes	3	Yes	1	Yes
3	Yes	4	Yes	2	Yes
4	Yes	4	Yes	2	Yes
5	Yes	5	Yes	1	Yes
6	Yes	4	Yes	2	Yes
7	Yes	5	Yes	1	Yes
8	Yes	5	Yes	1	Yes
9	Yes	4	Yes	1	Yes
10	Yes	4	Yes	2	Yes

Table 2: Measurement for Test Case 2

D. ANALYSIS

There are two types of messages that are transmitted in the TwiddleNet system. The first type of message is the Alert message. The Alert message contains the Meta data of the picture captured by the mobile client and is used to broadcast to clients that are subscripted to it. The second type of message is the image file. This image file can be downloaded from the content provider to the clients that have received the alert message. Figure 3 shows that the time taken for Client B to receive the Alert Message is about the same for both test cases. This is because the Meta data is only a few kilobytes and it does not cause a significant delay when transmitting through the TNT radio link. However, Figure 4 shows that the time taken to download the picture is about double for Test Case 1 as compare to Test Case 2. This is because the size of the image file is a few hundred kilobytes. However, the timing for Test Case 2 is still acceptable, as the average time taken is only 3.3 seconds.

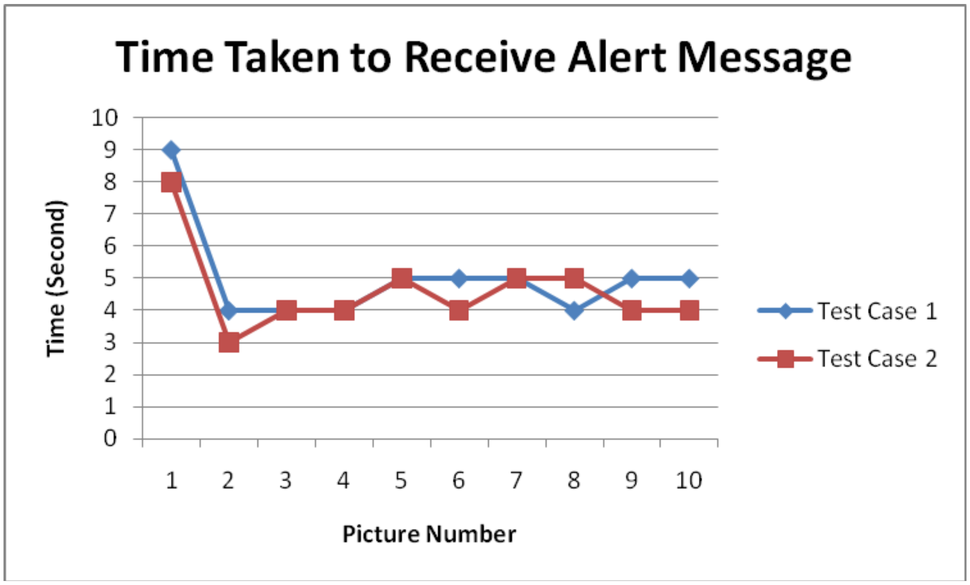

Figure 3: Time Taken to Receive Alert Message for Test Cases 1 and 2

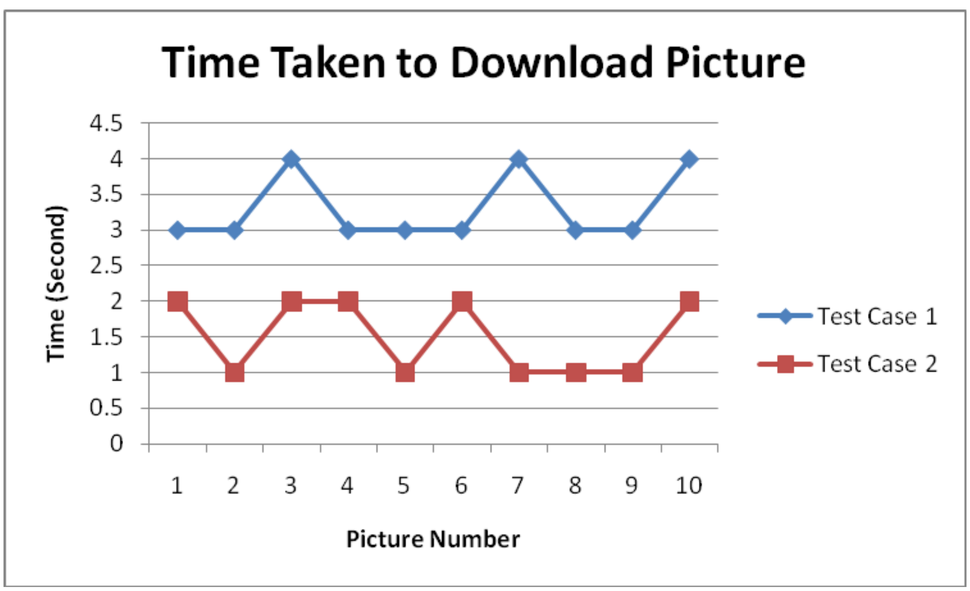

Figure 4: Time Taken to Download Picture for Test Cases 1 and 2

E. ISSUES ENCOUNTERED

As in any test that involves the complicated configuration of equipment and a constricted timeline, a failure in any of an assortment of areas would have a negative impact on our ability to complete a test that would prove the ability of TwiddleNet to operate over more than one wireless network. We had scheduled 17 and 18 of November for our testing with the actual conduct of our test expected to only take approximately two, hours under moderately stable conditions. Upon arrival and due to the limited experience that the operators of the tactical radios had (the radios had just recently been released), the radio network upon which our plan depended was not operational. This restricted our testing on the 17th to only operating on one wireless network. This did give us a chance to operationally check our equipment after transporting it over one hundred miles, but did not allow us to evaluate anything that TwiddleNet hadn't already shown it was able to perform. Difficulties with the radio network continued until early in the afternoon on the 18th (the day we planned to leave), and in the interim, we attempted to construct a wired network that would simulate what we had planned to operate under with the use of the tactical radios. This effort proved to be very difficult as we were competing with a simultaneous effort that continued its efforts to troubleshoot the radio network, and our wired efforts were continually interrupted in deference to testing the radio network.

Early in the afternoon of the 18th, the radio network became operational and at this point we were able to begin attempts to evaluate our testing. The initial plan was to use three subnets for the testing. The system, however, was unable to communicate through the Subnet Area 2 access point, possibly due to the incompatibility of the TwiddleNet data communication with the wireless access point. Due to time constraints, at this time we changed the test plan to perform the testing using only Subnet Areas1 and Area 3. These efforts proved viable and our results and conclusions are based on testing that utilized two wireless networks.

F. CONCLUSION

Our original test, as scripted, called for the transfer of communication across three different networks. The design of the test, however, was formulated based on the architecture at Camp Roberts. The real objective of our testing was to verify that TwiddleNet could simply perform content sharing across TWO networks. Our testing in this regard was successful and the test data supports this. Had the radio network at Camp Roberts been operational earlier, or if our team had more time to troubleshoot our issues with the third network, it is very likely that the test could have been performed successfully as designed.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] G. Sing, “Hastily Formed Networks for First Responders,” presented at 13th ICCRTS: C2 for Complex Endeavors, Bellevue, WA, 2008.

[2] Peter. J Denning, “Hastily Formed Network,” COMMUNICATIONS OF THE ACM April 2006/Vol. 49, No. 4.

[3] MWC Research Group (2009), “Military Wireless Communications (MWC) Research Group TNT CBE 10-1 After Action Report,” After Action Report.

[4] Christopher T. Clotfelter, and Jonathon E. Towle (2007), “TwiddleNet: Metadata Tagging and Data Dissemination in Mobile Device Networks,” M.S. thesis.

[5] Dirk Ableiter (2008) “Smart caching for efficient information sharing in distributed information systems,” M.S. thesis.

[6] Wikipedia, “IEEE 802.11,” http://en.wikipedia.org/wiki/IEEE_802.11 accessed on 1 October 2009.

[7] Jani Ilkka, Carlo Vainio, Nokia (2007) “Nokia Mobile Web Server” http://mymobilesite.net/files/MobileWebServer_Book_en.pdf accessed on 10 October 2009.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Professor Yeo Tat Soon
   Directory Of Temasek Defence System Institute
   National University of Singapore, Singapore

4. Tan Lai Poh
   National University of Singapore, Singapore

5. Sim Chey Hock
   FMS students: Civilian, Naval Postgraduate School
   Monterey, California

6. Lee Hong Aik
   FMS students: Civilian, Naval Postgraduate School
   Monterey, California